Hybrid Image Cryptosystem Based on Dyadic Phase Displacement in Frequency Domain

Yi C. Chang,[1,2] *Hsuan T. Chang,*[3] *& Chung J. Kuo*[4]

[1]Signal and Media (SAM) Laboratory
Department of Electrical Engineering
National Chung Cheng University

[2]Department of Electronic Engineering
Wu-Feng Institute of Technology

[3]Photonics and Information Laboratory
Department of Electrical Engineering
National Yunlin University of Science and Technology

[4]R&D Center, Components Business Group
Delta Electronics, Inc.

Abstract

Dyadic displacements of an image can be regarded as a special type of permutations of pixel addresses. This property can be used to encrypt an image and obtain perfect decryption. In this paper, a hybrid image cryptosystem based on the holographic interference and dyadic permutations is proposed. First, the phase and amplitude of the Fourier transform of an input image are recorded as the intensity information through the holographic interference. Then the extracted phase is processed through dyadic permutations by applying the exclusive-OR (XOR) operations on a user key and the addresses of all phase information. In decryption, an asymmetric process is used to recover the original image. Simulation results are provided to verify the proposed cryptosystem and show that the proposed scheme is robust to additional noise.

Subject terms: optical security, dyadic permutations, image cryptosystem, XOR operation, holographic interference, phase encryption.

January 2, 2004

1 Introduction

Optical security systems based on the optical signal processing and computing techniques recently have received a great deal of attention [1], [2]. The properties of the high-speed calculation and two-dimensional (2-D) parallelism make the optical security system more suitable to be employed in the practical security systems. Moreover, the optical security systems can provide higher security than digital systems because the optical components such as the holograms and phase-only masks are hard to be broken or duplicated.

Some optical security techniques based on holographic interference, such as the computer-generated hologram (CGH) interference [3] and the phase-shift method [4], have been elaborated. Because the CGH has no internal regularity and is hard to be duplicated, and the implementation of the holographic interference is not difficult, the security and encryption performance of these methods are very promising. However, these methods still have some drawbacks. In conventional random phase-encoding methods, for example, the double random phase encoding techniques [5]–[7], an image is encrypted with both the spatial and the frequency domains by the employment of randomly generated phase-only masks. Thus a frequency-domain filter is needed during the decryption process. In addition, high alignment accuracy is also required.

Recently, Castaneda et. al. [8] proposed an encryption technique, which employs the dyadic permutation on the image pixeles. The dyadic permutation is done by performing the exclusive OR (XOR) operations for the key and the addresses of the image pixels. With a proper selection of the key, the pixels in an image can be re-arranged such that the image can be encrypted as a very different one. However, there exist some disadvantages in this technique. First, the encrypted images can be similar to the original one when the keys used for dyadic operation are not carefully selected. Second, this encryption method is easy to be broken by the use of the brute force method when the size of plain image is known in advance. Finally, the optical implementation of the dyadic permutation should be pointed out in order to obtain higher operation speed. Therefore, we here propose the encryption method that can conquer the problems above.

XOR operation has some useful properties such as the closure and the reversibility, it has been used for optical image encryption in Ref. [9]. In this paper, an image encryption method based on optical holographic interference and the dyadic permutations in the frequency domain is proposed. First, an image is processed by means of Fourier transform and the holographic interference (with a plane reference wave). In the proposed cryptosystem, the amplitude of the Fourier transform of the input image and the intensity of the reference wave should be determined in advance. Then the phase part of the Fourier transform of the input image can be extracted by digital ways. The XOR operation is used to exchange the address of each pixel in the phase part and proceed to the encryption of the information system. This method provides advantages in design, fabrication, robustness for additive noise, and lower alignment requirement. Therefore it has a promising future in practical applications.

The remainder of this paper is given as follows: Section 2 gives the background of this work, which includes the hologram interference and the dyadic operation for Fourier phase. The motivation and the proposed method are described in Section 3. The computer simulation of the proposed method, the discussion on the effects of additive noise, and the possible optical implementation are given in Section 4. Finally, Section 5 concludes this paper.

2 Background

2.1 Hologram Interference

The experiments performed by Abbe and Porter [10] provide a powerful demonstration of the detailed mechanism by which coherent images are formed, and indeed the most basic principles of Fourier analysis itself. Owing to the experiments above, we can know that the Fourier spectrum of an input image appears in the back focal plane of the imaging lens. The discrete Fourier Transform pair can be expressed as follows:

$$F_O(u,v) = \frac{1}{N}\sum_{x=1}^{N}\sum_{y=1}^{N} f_O(x,y)e^{-i2\pi(ux+vy)/N}, \tag{1}$$

$$f_O(x,y) = \frac{1}{N}\sum_{x=1}^{N}\sum_{y=1}^{N} F_O(u,v)e^{i2\pi(ux+vy)/N}, \tag{2}$$

where $f_O(x,y)$ is an input image with $N \times N$ pixels and $F_O(u,v)$ is the discrete Fourier transform of $f_O(x,y)$. Each pixel of the input image $f_O(x,y)$ only has the amplitude information (real grayscale values), but its Fourier transform $F_O(u,v)$ has not only the amplitude but also the phase information. Hence we can rewrite Eq. (1) as follows:

$$F_O(u,v) = O(u,v)e^{-i\phi(u,v)}, \tag{3}$$

where $O(u,v)$ and $\phi(u,v)$ denote the amplitude and the phase parts, respectively.

If we place a charge coupled detector (CCD) sensor in the back focal plane of the imaging lens, then the CCD sensor responds only to light intensity $|O(u,v)|^2$. We can use a plane reference wave $R_O = Re^{-i\theta(u,v)}$ to assist the CCD sensor in detecting the phase of the Fourier transform $F_O(u,v)$, as shown in Fig. 1. The intensity I detected by the CCD sensor is given as follows:

$$I \propto |F_O + R_O|^2 = |O|^2 + |R|^2 + |O|\,|R|\,e^{i(\phi-\theta)} + |O|\,|R|\,e^{i(\theta-\phi)}. \tag{4}$$

Hence, we can rewrite Eq. (4) as follows:

$$cI(u,v) = |O|^2 + |R|^2 + 2\,|O|\,|R|\cos(\phi-\theta), \tag{5}$$

where c is a constant, which is inversely proportional to the sensitivity of the CCD sensor. In Eq. (5), the first two terms depend only on the intensities of the individual waves, the third term depends on their relative phase and amplitude information. For the encryption system, the magnitude $|O|$ of the Fourier transform of the input image, the intensity $|R|$, and the angle θ of the plane reference wave R_O can be determined in advance. Therefore, the phase part of the Fourier transform of the input image can be determined as follows:

$$\phi(u,v) = \cos^{-1}(\frac{cI - |O|^2 - |R|^2}{2\,|O|\,|R|}) + \theta. \tag{6}$$

2.2 Dyadic Displacement of Fourier Phase

A digitized image, for example, that captured by a CCD sensor or analyzed by a digital image processing device, can be represented as a 2-D digital function $f(n,m)$. It can be defined as an array of $N \times M$ pixels. Both the indices n and m denote the addresses of the function values, and $n = 0, 1, \ldots, N-1$ and $m = 0, 1, \ldots, M-1$.

Performing the XOR operation with binary digits $j \in [0, N-1]$ and $k \in [0, M-1]$, respectively, on the addresses of a 2-D function, i.e. $f(n,m) \rightarrow f(n \oplus j, m \oplus k)$, is called the dyadic displacement of that function [11]. It exhibits the following properties:

1. **Closure:** The new addresses will have the same number of bits as the original ones.

2. **One-to-one mapping:** If a set of data $0, 1, 2, 3$ is processed by the XOR operation, for example the binary-digit representation of the key is 01, then the result is shown as follows:

   $$00 \oplus 01 = 01; 01 \oplus 01 = 00; 10 \oplus 01 = 11; 11 \oplus 01 = 10.$$

   Both the domain and the region are within the same range [0, 3]. Therefore, if an image is processed by the XOR operation, then the processed image will have the same amount of pixels as the original one.

3. **Reversibility:** Each original address can be recovered by the XOR operation of the corresponding encrypted address using the correct key, because

   $$(x \oplus \text{key}) \oplus \text{key} = x.$$

3 Proposed Method

3.1 Motivation

Owing to the properties shown in the previous section, dyadic displacements can be used as a simple but useful encryption procedure. It can recover the original image without information loss or degrading [12] because nothing is added to perform the encryption. While the dyadic displacement has these advantages above, however, the encryption system [8] that only employed the dyadic displacement on the image pixels has two fatal drawbacks. First, the encrypted results may not be random enough to conceal the original information when the transition number of 1 and 0 within binary digits of the user key is few. The transition number (the change number in bits) of a key of 8 bits, for example, $(64)_{10} = (01000000)_2$, is 2 because there are two bit changes in its binary representation. That is, 0→1 and 1→0 from the first bit to the third bit. There are no transitions in the following bits because they are all 0s. The possible transition numbers of a key of n bits are 0, 1, 2, ..., n-1. The transition number dominates the permutation result of the Lady image. The scrambling effect is better for a key with a larger transition number. This phenomenon has been demonstrated in Figs. 2(a)–2(d), in which the transition numbers of the four keys $(0)_{10} = (00000000)_2$, $(255)_{10} = (11111111)_2$, $(64)_{10} = (01000000)_2$, and $(85)_{10} = (01010101)_2$ are 0, 0 , 2, and 7, respectively. Obviously, the Lady image of size 256×256 (shown in Figs. 2(a)) is very difficult to be recognized from Fig. 2(d) (key = 85), because the transition number of the user key is the largest. However, the images shown in Figs. 2(b) and 2(c) are very easy to be recognized, in which the transition numbers are only zero and two, respectively. Furthermore, each user key is set by individual user and cannot be controlled by the encryption system.

Second, the encrypted image can be easily broken. For example, let the Lady image be encrypted based on the dyadic displacement with the user key 85. If someone inputs the keys that are similar to the user key in the bit-plane format, then the output may be some recognizable images such as that shown in Figs. 3(a)–3(c). The figures shown in Fig. 3(a)-3(d) are the results for the input keys 86, 84, 170, and 64, which their Hamming distances to the correct user key 85 are 2, 1, 1, and 3, respectively. If the size of an image is known in advance, then the bit length l of the key can be determined. Thus the correct key can be easily found by the use of the brute force method, in which all the possible keys with the same bit length are tested such that the original image can be discovered. Here we point out some observations as follows:

1. The encrypted image can be very different from the original one only when the user key is with a large transition number.

2. The less Hamming distance between the user key and the input key is, the less difference between the decrypted and the original images can be obtained.

3. If the input key and the user key are complementary (the sum of the input key and the user key is equal to $2^l - 1$), then the decrypted image is the 180° rotated version of the original one.

Figure 4(a) and 4(b) shows the logged MSE results versus the transition number and the Hamming distance, respectively, for all the possible user keys in this method. As shown in 4(a), the transition numbers of the user keys are within the range [0,7] and the smaller MSE values of the encrypted images are obtained for smaller user keys. However, as shown in Fig. 2(b), which is just an overturned version of the original image, some of the encrypted images may be easily recognized although they are of large MSE values. Therefore, the number of useful user keys actually is less than 255. On the other hand, consider Fig.

4(b). Even a suitable user key is chosen, the MSE values of the input keys that are close to the user key are smaller than that of other input keys. Two examples shown in 3(a) and 3(b) verify this result.

According to the observations shown above, it is unwise to encrypt an image by directly applying the dyadic permutation on the image pixels. Therefore, we here propose a hybrid cryptosystem that can perform the dyadic permutation in the frequency domain. Because the rearranged phase information has to be re-transformed into the spatial domain, the recovered image can still be very different from the original one. Therefore, the selection of the user key is not so critical in the proposed cryptosystem. In addition to the phase information, higher security can be achieved when the amplitude information and the parameters used in the holographic interference, such as the angle incident to the hologram plane, can be considered simultaneously.

3.2 Encryption

The block diagram and the optical architecture of the encryption procedure of the proposed cryptosystem are shown in Fig. 5(a) and Fig. 6(a), respectively. First, the input image is optically Fourier transformed. This procedure can be easily implemented by optics, which is shown in the upper part of Fig. 6(a). The Fourier spectrum is detected by a CCD sensor and then transmitted to a computer for further digital processing. The computer determines the magnitude part of the Fourier transform as the first key, i.e., $key_1 = |F_o(u,v)|$. On the other hand, a reference wave is incident on the detection plane with an oblique angle θ. The interference pattern of the Fourier transform of the input image and the reference wave is obtained as shown in Eq. (4). From Eq. (6), the computer in Fig. 6(a) can determine the phase information $\phi(u,v)$ of the Fourier transform of the input image because that the intensity of the Fourier transform of the input image, $|O|^2$, the intensity of the plane reference wave, $|R|^2$, can be determined in the encryption system in advance.

The extracted phase $\phi(u,v)$ is within the range $[-\pi,\pi]$. For the purpose of convenient storage and transmission, the extracted phase is mapped to the grayscale value within the range [0, 255]. There are many mapping ways between the phase and the grayscale values. For example, the grayscale value $\phi_m(u,v)$ can be determined as

$$\phi_m(u,v) = \lfloor 255 \times \frac{\phi(u,v)+\pi}{2\pi} \rfloor, \tag{7}$$

where $\lfloor\cdot\rfloor$ denotes the floor operation for finding the largest integer. **Then the computer in Fig. 6(a) performs XOR operations for the addresses of the mapped phase $\phi_m(u,v)$ and the user key, key_{user}, in eight bit planes. That is,**

$$key_{\text{user}} = \cup_{i=1}^{8} key_{\text{user}}^{(i)}, \tag{8}$$

and

$$\phi_e^{(i)}(u,v) = \phi_m^{(i)}(u \oplus key_{\text{user}}^{(i)}, v \oplus key_{\text{user}}^{(i)}), \quad \text{for} \ \ i = 1,2,\ldots,8, \tag{9}$$

where $\phi_e^{(i)}(u,v)$ and $\phi_m^{(i)}(u,v)$ denote the i^{th} bit of $\phi_e(u,v)$ and $\phi_m(u,v)$, respectively. By combining the $\phi_e^{(i)}(u,v)$ in the eight bit planes, the result of dyadic permutations of the mapped phase, $\phi_e(u,v)$, can be obtained. In the proposed cryptosystem, this encrypted phase $\phi_e(u,v)$ serves as the second key key_2. To obtain higher security, two user keys, one for u address and the other for v address, can be used. Moreover, the oblique angle θ can also be varied during the determination of the phase $\phi_m(u,v)$. In such a case, the computer will determine another information that can be used to design the second key. Here the oblique angle θ is jointly considered with the phase $\phi(u,v)$. That is,

$$\cos[\phi(u,v)-\theta] = \frac{cI - |O|^2 - |R|^2}{2|O||R|}. \tag{10}$$

Similarly, this value within the range $[-1,1]$ is mapped to the grayscale value within the range $[0,255]$. Thus a higher security of the system is obtained, because anyone that even possesses both keys, key_1 and key_2, cannot reconstruct the original information without the information regarding to the angle θ.

3.3 Decryption

The block diagram and the optical setup for the decryption system are shown in Fig. 5(b) and Fig. 6(b), respectively. Each user must possess key_1, the Fourier spectrum of the original image, key_2, which corresponds to the encrypted phase information, the correct user key, and the angle θ, simultaneously. Moreover, both keys key_1 and key_2 must be placed at the correct positions, then the correct user key can be used to decrypt the original image.

The key key_2 in the grayscale form cannot be directly used to recover the original image. It should be converted into the phase form in the computer and then the dyadic operations are applied to reconstruct the original phase information. In Fig. 6(b), the key key_2 is placed in front of the CCD sensor such that the intensity detected by the CCD sensor is given as follows:

$$\phi_d \propto \phi_e, \tag{11}$$

which corresponds to the grayscale values shown in the key key_2 (the encrypted phase information of the Fourier transform of the original image). Hence, we can rewrite Eq. (10) as follows:

$$\phi_d = c_d \phi_e, \tag{12}$$

where c_d is a constant coefficient that is in proportion to the sensitivity of the CCD sensor. For the CCD sensor shown in Fig. 6(b), the coefficient c_d does not need to be known in advance. The angle of the pixel with the maximal value captured by the CCD sensor in Fig. 6(b) is equal to π for sure. With a proper scaling factor, the angles of other pixels can be computed from Eq. (10). Then the computer shown in Fig. 6(b) proceeds the dyadic permutations with the user key to yield the phase $\phi_p(u, v)$. If both the input key and the angle θ are correct, then the phase $\phi_p(u,v)$ should be identical to the phase $\phi(u,v)$ of the Fourier transform of the original image. With the optical Fourier transform, the original image will appear and can be detected in the back focal plane of the Fourier-transform lens shown in Fig. 6(b).

3.4 Level of Security

Suppose that an unauthorized user owns the amplitude information (key_1) and the scrambled phase information (key_2). Then the number of the possible combination becomes $256^8 = 2^{64}$ and the user key is 64-bit long now. To increase the security degree, we can use two different user keys for u and v addresses at each bit plane. Then the number of combination then becomes $(256^2)^8$=$2^{128} \approx 3.4028 \times 10^{38}$, which should be secure enough, and the user key is 128-bit long. As to the amplitude information, another user key(s) may be applied using the same operation as that for the phase information. On the other hand, the incident angle θ of the reference wave also can contribute the security degree of the proposed cryptosystem.

To further increase the level of security, different ways of the phase-to-amplitude mapping shown in Eq. (7) can also provide more protection. Furthermore, the proposed method can cooperated with the double random phase encoding techniques [6]. Two random phase masks can be used to further encrypt the amplitude and phase information. In addition to the user key, breaking two random phase masks will be much more difficult for the unauthorized users.

4 Simulation and Discussion

In computer simulation, the Lady and Pattern images of size 256×256 are used to test the proposed cryptosystem. To simplify the comparison with the method shown in Section 3.1 and easily demonstrate the effectiveness of the proposed method, here the results of using only the 8-bit-long user key on the pixel addresses are performed. Figure 7(a) shows the Fourier spectrum of the Lady image. The mapped phase $\phi_m(u,v)$ of the Fourier transform is shown in Fig. 7(b). Figures 7(c) and 7(d) are the encrypted results that the mapped phase $\phi_m(u,v)$ is processed with the user keys 64 and 85, respectively. That is, $\phi_e(u,v) = \phi_m(u \oplus 64, v \oplus 64)$ and $\phi_e(u,v) = \phi_m(u \oplus 85, v \oplus 85)$. Though the transition number of the user key 64 is only 2, the original image cannot be recognized from Fig. 7(c). Hence, the first problem about the limited selection of the user key in the encryption system that only employed the dyadic displacements on image pixels can be solved in the proposed method. After the decryption, both the mean-square error (MSE) and the peak-signal-to-noise ratios (PSNRs) of the recovered image f' are used to represent the quality. The MSE and PSNR of a recovered image are defined as

$$\mathrm{MSE}(f,f') = \frac{1}{N^2}\sum_{x=1}^{N}\sum_{y=1}^{N}[f(x,y) - f'(x,y)]^2, \tag{13}$$

and

$$\mathrm{PSNR} = 10\log_{10}\frac{255^2}{\mathrm{MSE}} \ \ \mathrm{dB}, \tag{14}$$

respectively. For the Lady image, the recovered image is with the MSE 0.77 and the PSNR 47 dB. That is, the image fidelity in the proposed cryptosystem is well preserved.

Because the Pattern image has some easily recognized shapes, it is used to test the proposed cryptosystem. Figure 8(a) shows the mapped phase $\phi_m(u,v)$ of the Fourier spectrum of the Pattern image. The encrypted phase $\phi_e(u,v)$, with the user key 85, of the mapped phase $\phi_m(u, v)$ is shown in Fig. 8(b). Figures 8(c) and 8(d) are the decrypted results of using the input keys 86 and 84 when the user key is 85. From both figures and the corresponding MSE and PSNR values, the decrypted images obtained from the incorrect input keys are very different from the original image, even the input keys are very close to the user key. Hence, the proposed system can overcome the second problem.

Figures 9(a) and 9(b) demonstrate the effects of the transition number of the user keys and the Hamming distance between the user key and the input key, respectively. As shown in Fig. 9(a), for all possible user keys with different transition numbers, the MSE values of the decrypted image are equally large even when the input key is very close to the user key. Thus the selection of the user key is not limited by the transition number. As for the Hamming distance, Fig. 9(b) shows that only the user key can correctly decrypt the original image. Otherwise, large MSE values are obtained even the input keys are very close to the user key. The examples shown in Fig. 8(c) and 8(d) verify this result. Compared with the results shown in Fig. 4(a) and 4(b), the selection of the user key of the proposed method is independent on the transition number and robust to the input keys with low Hamming distances. Figure 10(a) shows the decrypted image when the input key is 170 and the user key is 85. Both keys are complementary because their sum is equal to 255. The original image cannot be recognized from Fig. 10(a). Moreover, Fig. 10(a) is not similar to the overturned original image at all. Hence, the proposed system can overcome this kind of problems in the encryption system that only employs the dyadic displacements on image pixels. For the proposed cryptosystem, the original image can be recovered only when the input key is equal to the user key. Figure 10(b) shows the correct recovered image whose quality is quite high. The MSE and PSNR of this image are 0.18 and 54.5 dB, respectively.

The effects of the amplitude information in the proposed cryptosystem are also considered here. Suppose that the correct phase information and the user key are obtained, but the amplitude information is lost. If the amplitude information is guessed as a constant such as 255 for each pixel value, the decrypted images for the Lady and Pattern images are shown in Fig. 11(a) and 11(b), respectively. Only some blur contour information can be observed from both figures and most of the information is lost. Therefore, the user key can also be applied to the amplitude information such that the higher security level can be achieved.

For the proposed cryptosystem, both keys, key_1 and key_2, are portable data. Both keys may be transmitted through the Internet or carried by someone to the decryption system. Hence, key_1 and key_2 may be interfered with some noise. Therefore, it is necessary to discuss the immunity against the noise for the proposed cryptosystem. Figures 12(a) and 12(d) show the decrypted Pattern images under that both keys key_1 and key_2 are corrupted by 15% additive 'salt and pepper' noise. Obviously, all the decrypted images still can be recognized and very close to the original one.

5 Conclusion

In this paper, we proposed a hybrid cryptosystem to encrypt an plain image by performing the dyadic permutation on the phase information in the frequency domain. The proposed method not only overcomes the drawbacks of the encryption system that only employed the dyadic displacements on image pixels, but also provides the advantage of the robustness to the additive noise. High degree of security can be furthermore achieved while cooperating with the double random phase encryption technique. Patrick [13] has presented a feasible optical implementation for the dyadic displacements. In the future, we will develop some parallel hardware to perform the computation, finding the maxima [14] and the dyadic displacements, to make the proposed system become a whole parallel structure. On the other hand, to obtain efficient transmission over the Internet or storage for both keys, the proposed system is still conducive to the compression of the information contained in the keys. This compression issue can be one of the important future research topics.

Acknowledgment

This work was partially supported by the National Science Council, Taiwan, under contract NSC 91-2215-E-224-007.

References

[1] J. Horner and B. Javidi, *Optical Engineering,* **35**(9), Special issue on Optical Security (1996)

[2] J. Horner and B. Javidi, *Optical Engineering,* **38**(1), Special issue on Optical Security (1999)

[3] Y. Guo, Q. Huang, J. Du and Y. Zhang, "Decomposition storage of information based on computer-generated hologram interference and its application in optical image encryption," *Applied Optics*, **40**(17), 2860–2863 (2001).

[4] S. Lai and M. A. Neifeld, "Digital wavefront reconstruction and its application to image encryption," *Optics Communications*, **178**, pp. 283–289 (2000).

[5] P. Refregier and B. Javidi, "Optical image encryption using input plane and Fourier plane random encoding," *Optics Letters*, **20**(7), pp. 767–769 (1995)

[6] B. Javidi and E. Ahouzi, "Optical security with Fourier plane encoding," *Applied Optics*, **37**(26), pp. 6247–6255 (1998)

[7] N. Towghi, B. Javidi, and Z. Luo, "Fully phase encrypted image processor," *Journal of Optical Society of America, A*, **16**(8), pp. 1915–1927 (1999)

[8] Roman Castaneda, Jorge Garcia-Sucerquia, Rodrigo Henao, and Osvaldo Trabocchi, "Information encryption through dyadic permutation," *Opt. and Laser in Eng.* **36**, 537–544 (2001)

[9] J.-W. Han, C.-S. Park, D.-H. Ryu, and E.-S. Kim, "Optical image encryption based on XOR operations," *Optical Engineering*, **37**(1), pp. 47–54 (1999)

[10] Joseph W. Goodman, *Introduction to Fourier Optics*, McGraw-HILL, chap. 8, pp. 218 (1996)

[11] K. G. Beauchamp, *Walsh functions and their applications*, London: Academic Press (1975)

[12] R. J. Clarke, *Transform coding of image*, New York: Academic Press (1985).

[13] Patrick Naulleau, "A coherence encoding method for optical switch, encryption, and arithmetic," *Optics Communications*, **189,** pp. 55–61 (2001).

[14] Yi C. Chang and Chung J. Kuo, "A novel Winner-Take-All network without iteration," *IEEE/ASME International Conference on Advanced Manufacturing Technologies and Education in the 21st Century*, pp. 61 (2002).

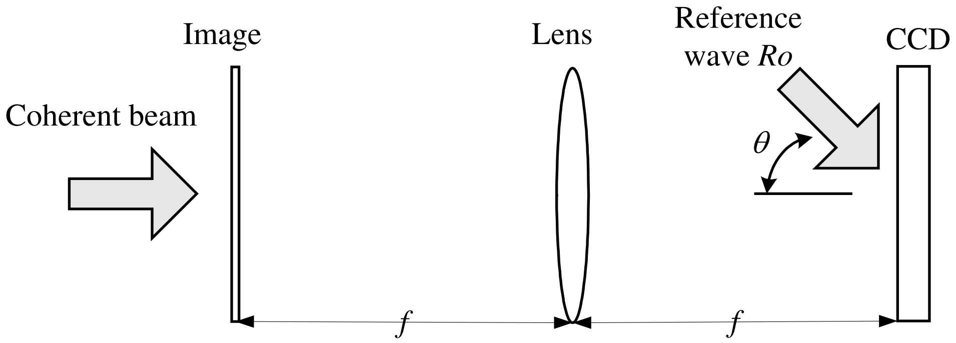


Figure 1: The optical setup of holographic interference.

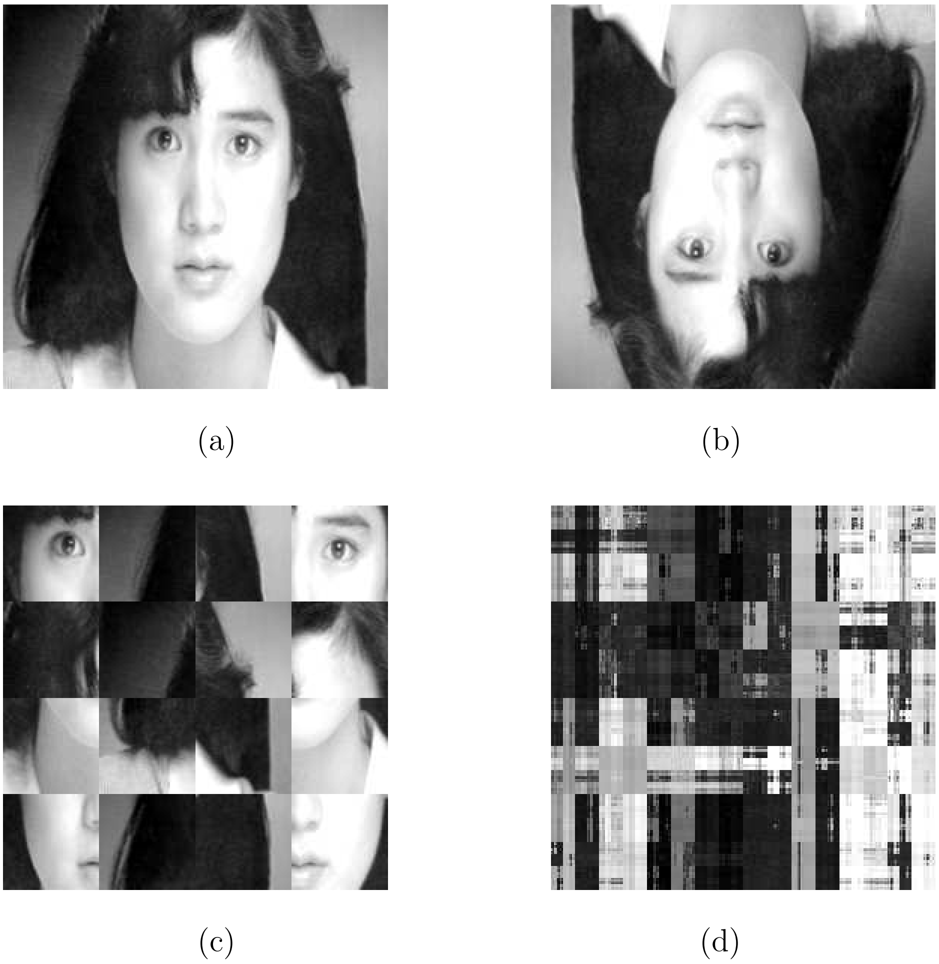
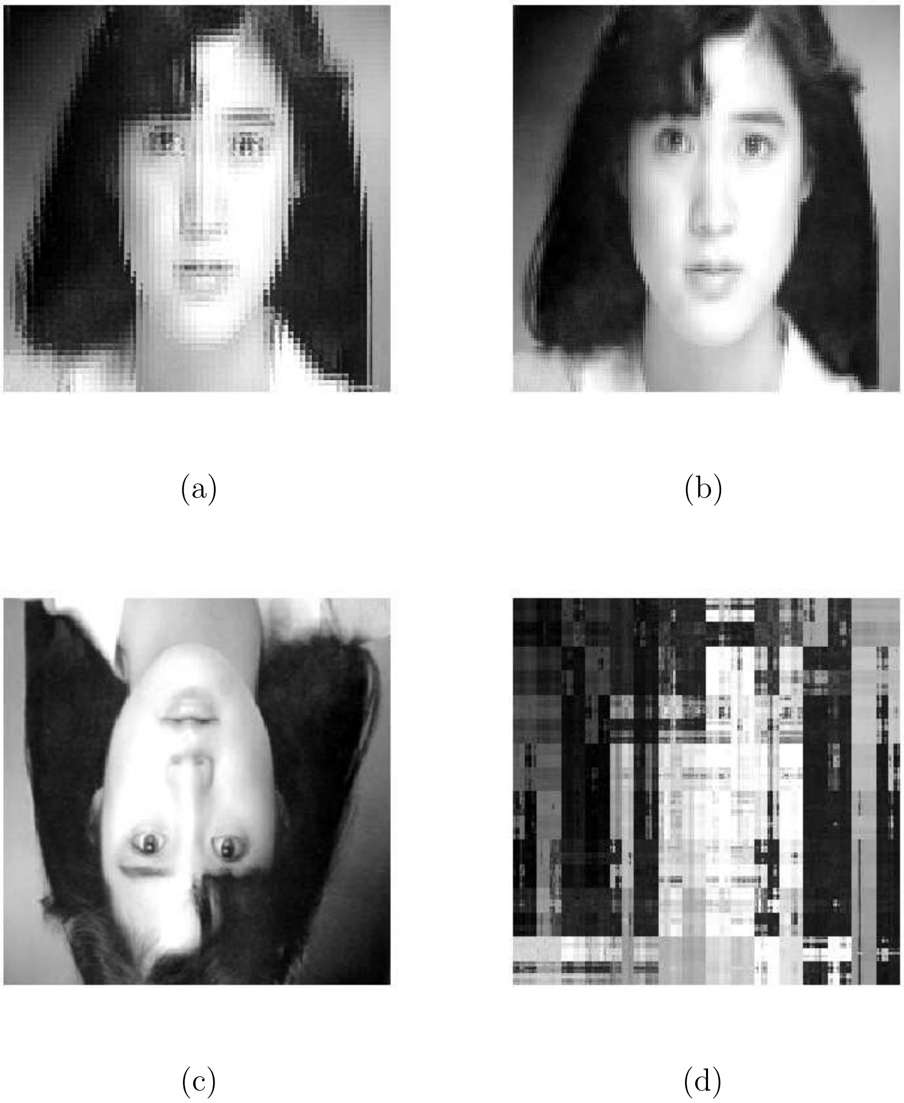


Figure 2: The results of that only the dyadic displacements on the pixels of the Lady image are used: (a) key = 0, (b) key = 255, (c) key = 64, and (d) key = 85.



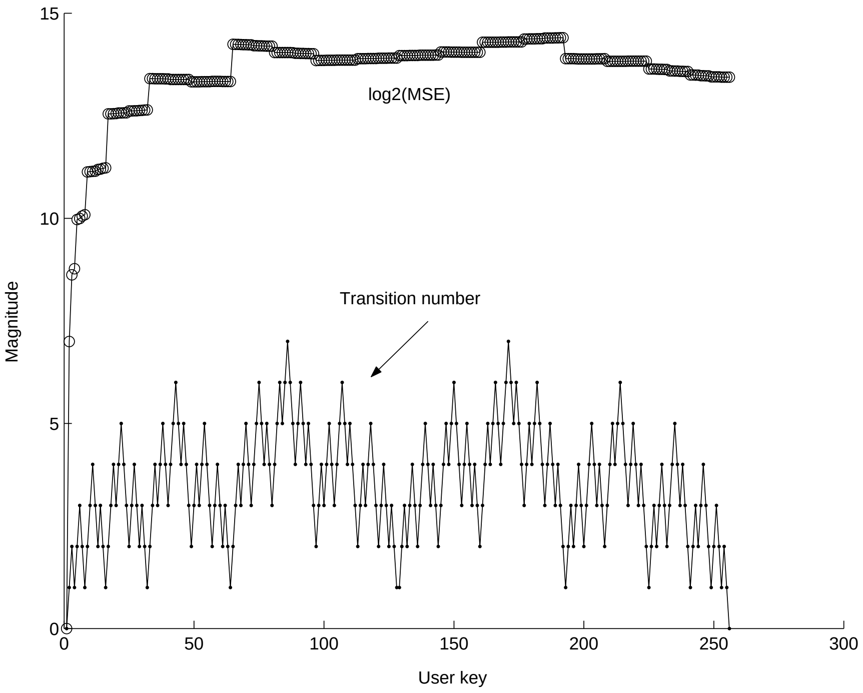
(a)

(b)

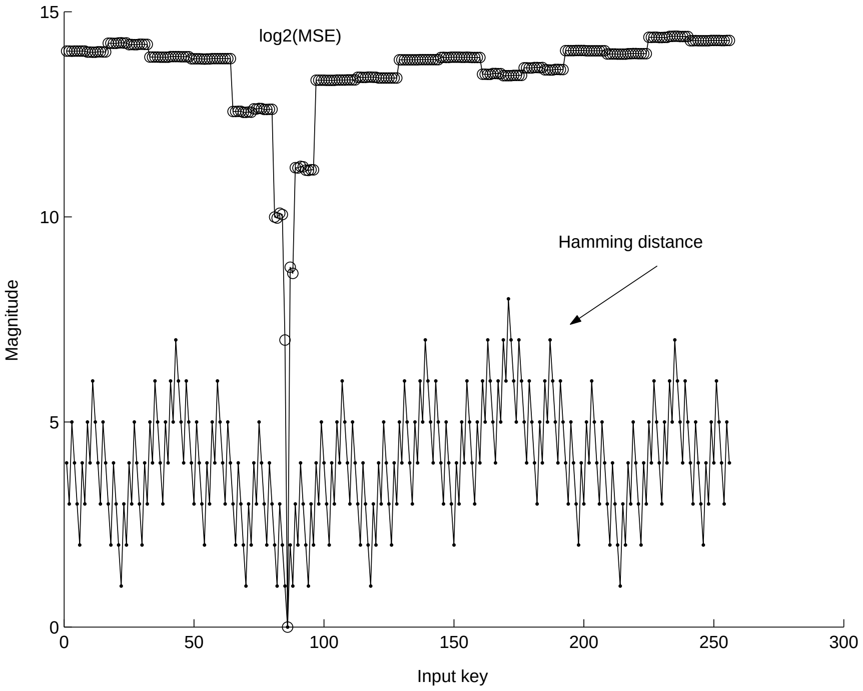
(c)

(d)

Figure 3: The decrypted results for the different input keys: (a) 86, (b) 84, (c) 170, and (d) 64. The correct user key is 85.



(a)



(b)

Figure 4: For the dyadic permutations that are directly performed on the pixels, (a) MSE versus transition numbers for all possible user keys; (b) MSE versus Hamming distances between all possible user keys and the correct user key ($key_{\text{user}} = 85$).

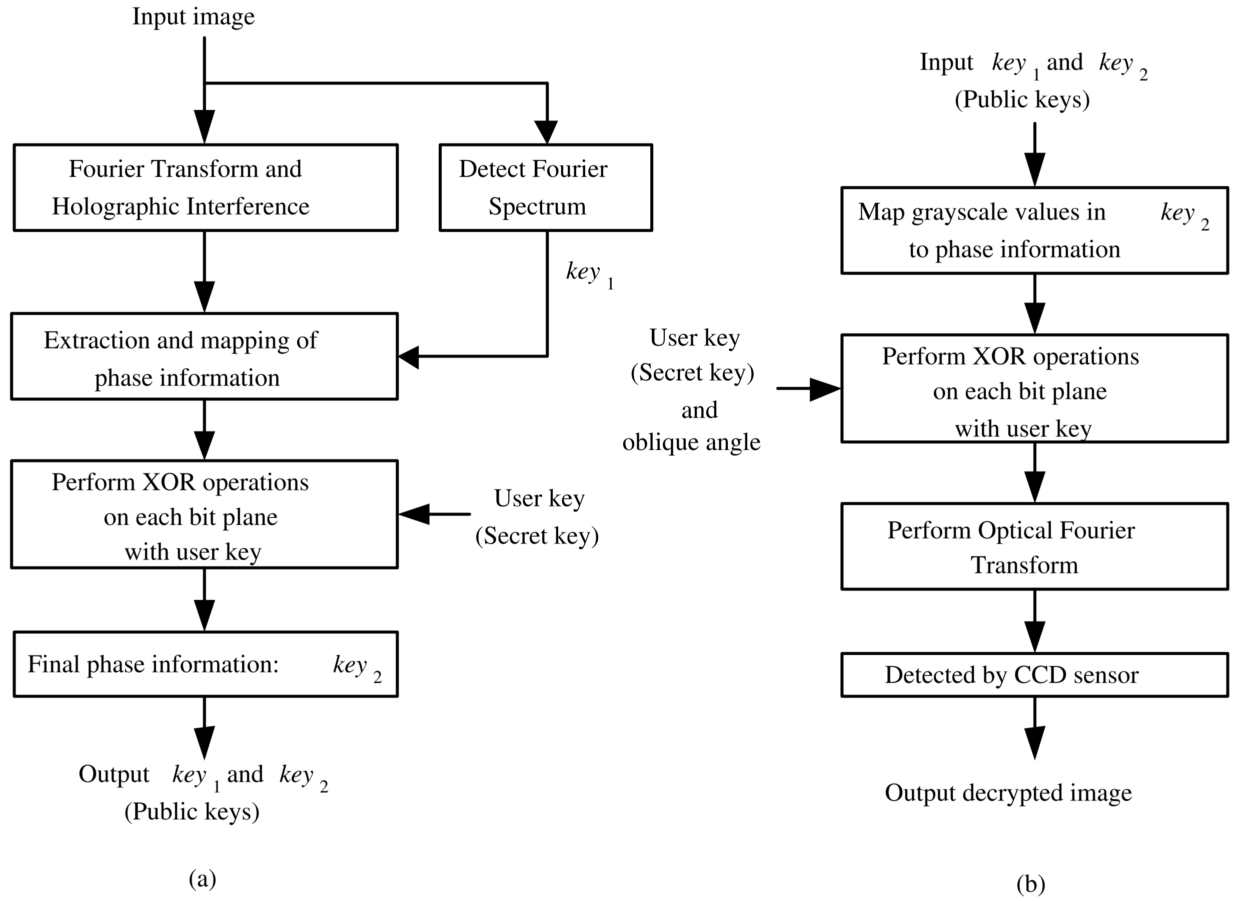

Input image
Fourier Transform and Holographic Interference
Detect Fourier Spectrum
key 1
Extraction and mapping of phase information
Perform XOR operations on each bit plane with user key
User key (Secret key)
Final phase information: key 2
Output key 1 and key 2 (Public keys)
(a)
Input key 1 and key 2 (Public keys)
Map grayscale values in key 2 to phase information
User key (Secret key) and oblique angle
Perform XOR operations on each bit plane with user key
Perform Optical Fourier Transform
Detected by CCD sensor
Output decrypted image
(b)

Figure 5: The block diagrams of the encryption and decryption processes in the proposed cryptosystem.

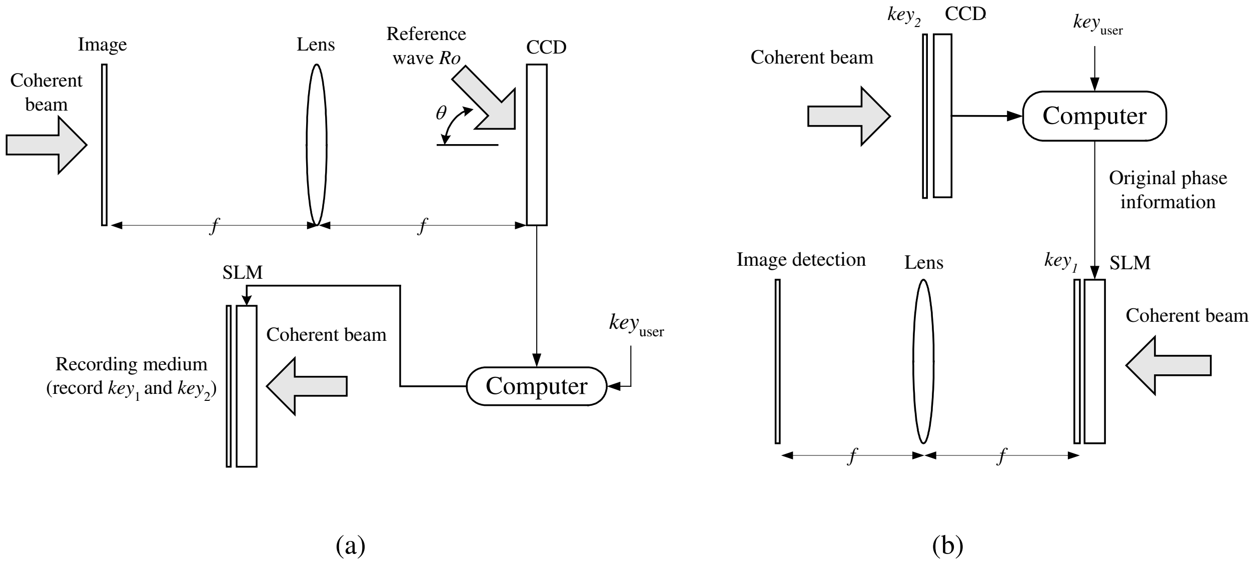
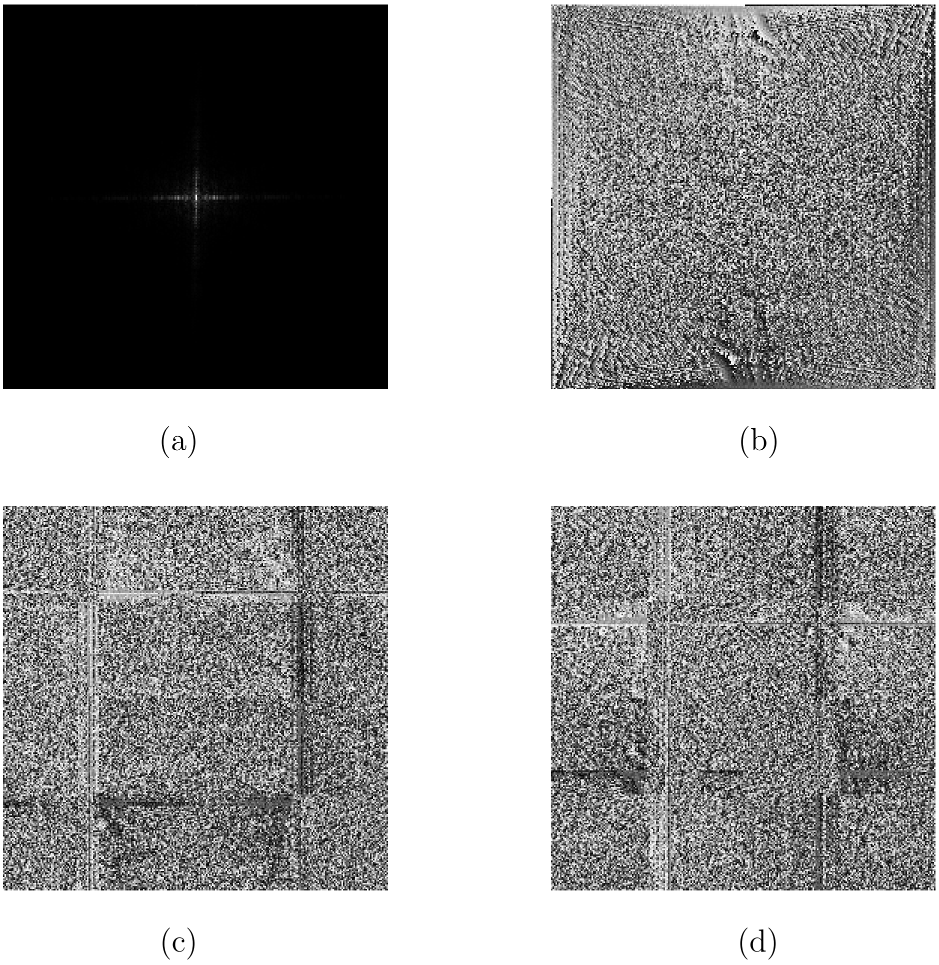


Figure 6: The optical setups of the proposed hybrid cryptosystem: (a) encryption and (b) decryption systems.



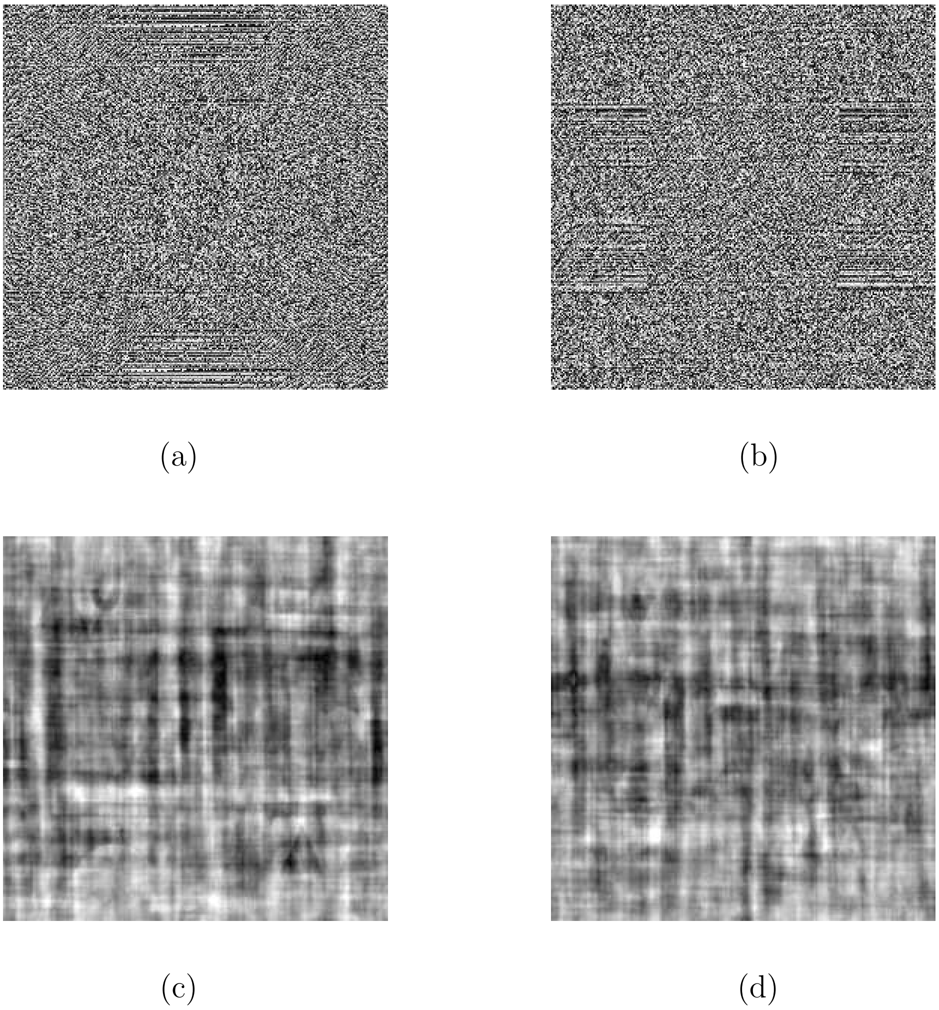
(a)

(b)

(c)

(d)

Figure 7: (a) The power spectrum of the original image. (b) The mapped phase represented as grayscale values. The encrypted phase information with user keys (c) $key_{\text{user}} = 64$ and (d) $key_{\text{user}} = 85$ for the Lady image.



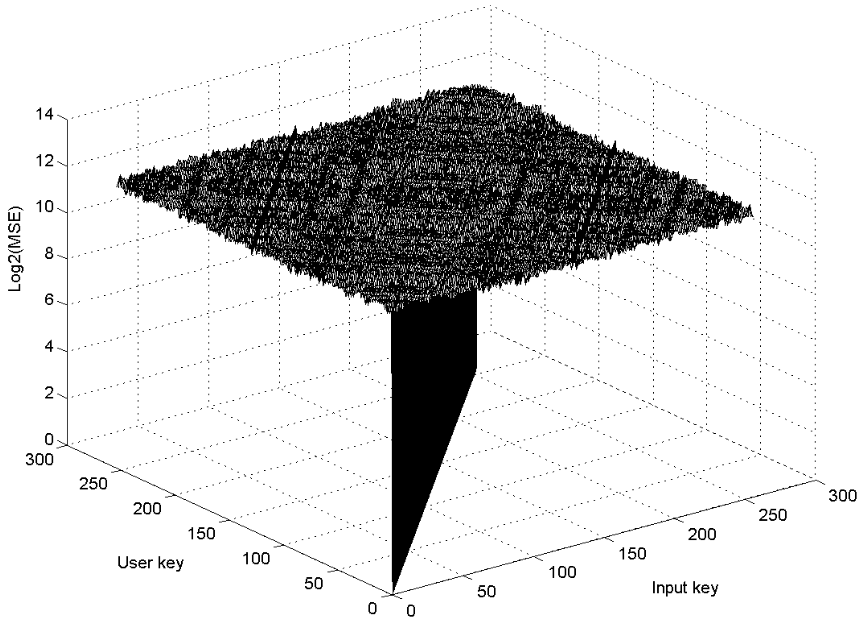
(a)

(b)

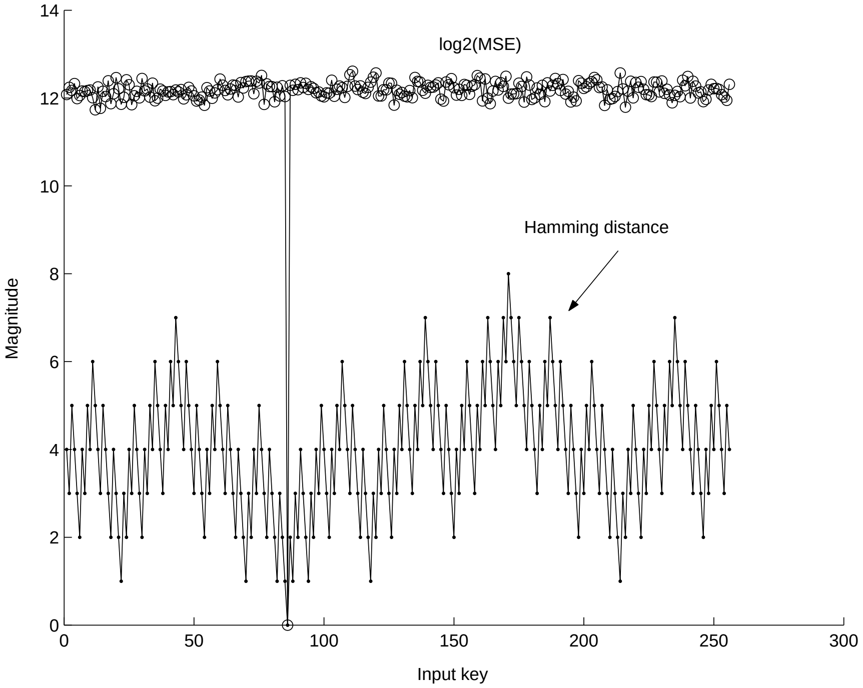
(c)

(d)

Figure 8: (a) The extracted phase, (b) the encrypted phase with user key=85. The decrypted images are with (c) $key_{\mathrm{user}} = 86$, MSE = 4592.8, PSNR = 11.51 dB and (d) $key_{\mathrm{user}} = 84$, MSE = 3936.2, PSNR = 12.18 dB, for the Pattern image.

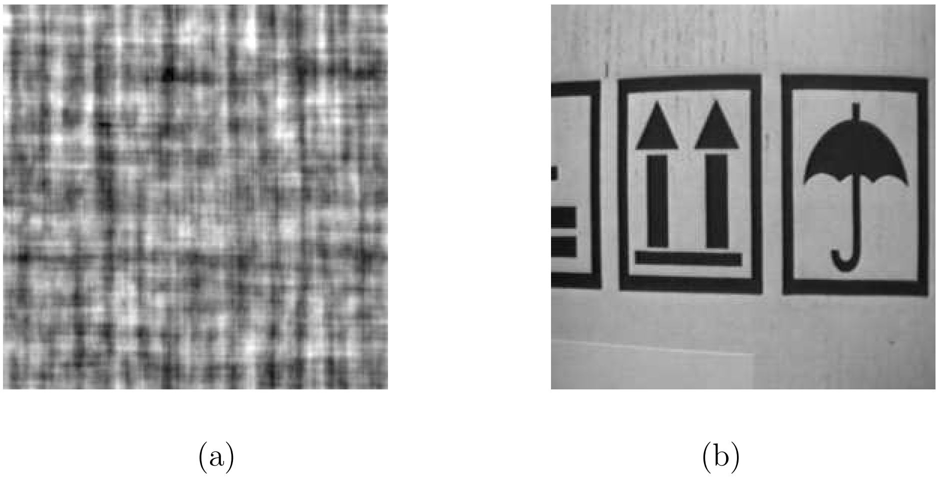


(a)



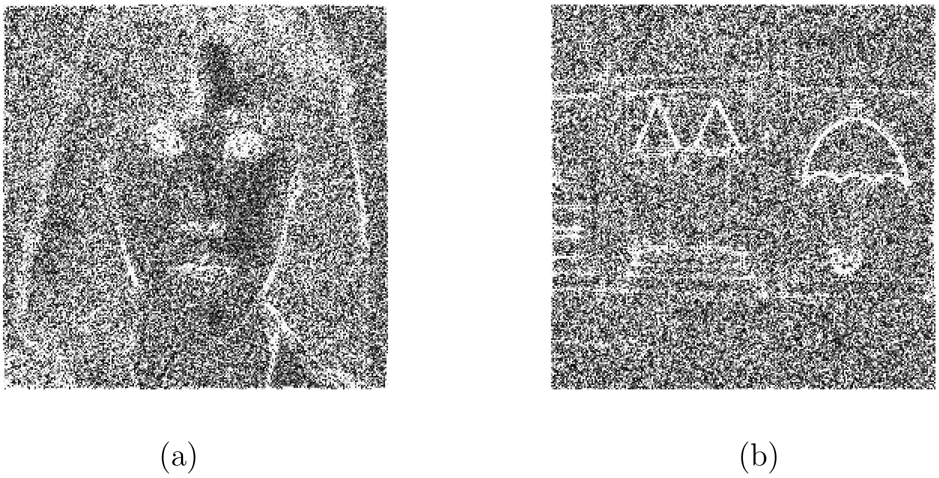
(b)

Figure 9: For the proposed method, (a) MSEs under different transition numbers for all possible input keys; (b) MSEs versus Hamming distances between all possible user keys and the correct user key ($key_{\text{user}} = 85$).



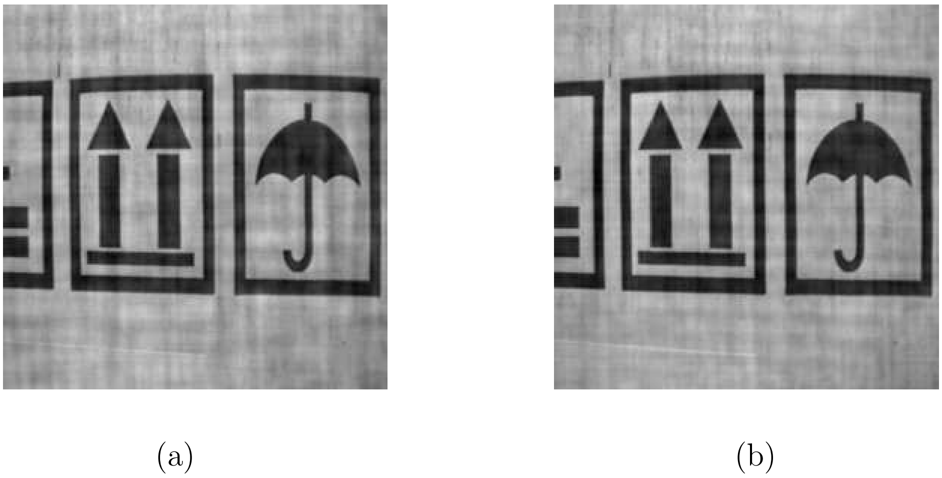
(a) (b)

Figure 10: The decrypted images for (a) the user key $key_{\text{user}} = 170$, MSE = 3733.2, PSNR = 12.41 dB, and (b) the correct user key $key_{\text{user}} = 85$, MSE = 0.1814, PSNR = 54.45 dB.



(a) (b)

Figure 11: The decrypted images with the correct user key, the phase information, but the incorrect amplitude information (the grayscale values in key_1 all are 255): (a) Lady image, (b) Pattern image.



(a)

(b)

Figure 12: The decrypted images with 15% additive‘salt and peppers’ noise for both keys: (a) key_1, MSE = 148.65, PSNR = 26.38 dB, (b) key_2, MSE = 814.86, PSNR = 19.02 dB.